ČESKÁ TECHNICKÁ NORMA

ICS 34.040 **Únor 2012**

Informační technologie – Bezpečnostní techniky – Nepopiratelnost – Část 1: Všeobecně

ČSN ISO/IEC 13888-1
36 9787

Information technology – Security techniques – Non-repudiation – Part 1: General

Technologies de l,information – Techniques de sécurité – Non-répudiation – Partie 1: Généralités

Informationstechnik – Sicherheitsverfahren – Nichtabstreitbarkeit – Teil 1: Allgemeines Modell

Tato norma je českou verzí mezinárodní normy ISO/IEC 13888-1:2009. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 13888-1:2009. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných normativních dokumentech

ISO/IEC 10181-4 zavedena v ČSN ISO/IEC 10181-4 (36 9694) Informační technologie – Propojení otevřených systémů – Bezpečnostní struktury otevřených systémů – Část 4: Struktura nepopiratelnosti

ISO/IEC 18014 (všechny části) dosud nezavedena

Souvisící ČSN

ČSN ISO/IEC 9798-1 (36 9743) Informační technologie – Bezpečnostní techniky – Mechanismy autentizace entit – 1. část: Obecný model

ČSN ISO/IEC 10118-1 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce – Část 1: Všeobecně

ČSN ISO/IEC 10181-1:1998 (36 9694) Informační technologie – Propojení otevřených systémů – Bezpečnostní struktury otevřených systémů – Část 1: Přehled

ČSN ISO/IEC 13888-2 (36 9787) Informační technologie – Bezpečnostní techniky – Nepopiratelnost – Mechanismy používající symetrické šifry

ČSN ISO/IEC TR 14516 (36 9791) Informační technologie – Bezpečnostní techniky – Směrnice pro používání a řízení služeb důvěryhodných třetích stran

Další informace

Pro anglický termín „time stamp“ (čl. 3.57) je pro účely této normy použit v souladu s terminologií zavedenou normou ČSN ISO/IEC 18014-1 český termín „vyznačení času“, a s ohledem na běžnou praxi je rovněž uveden další často používaný termín „časové razítko“.

Anglický termín symbol se překládá českým slovem symbol, protože se zde používá ve významu nadřazeného termínu vůči podřazeným termínům: značky, znaky, označení atd., aby se všechny tyto termíny nemusely vypisovat.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČ 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 13888-1
Nepopiratelnost – Třetí vydání
Část 1: Všeobecně 2009-07-15

ICS 35.040

Obsah

Strana

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1.

Mezinárodní normy jsou navrhovány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání návrhu jako mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědné za identifikaci libovolného patentového práva nebo všech takových patentových práv.

ISO/IEC 13888-1 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* sub-
komise SC 27, *Bezpečnostní techniky IT*.

Třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 13888-1:2004), které prošlo technickou revizí.

ISO/IEC 13888 se skládá z následujících částí se společným názvem *Informační technologie* –

Bezpečnostní techniky – Nepopiratelnost:

- *Část 1: Všeobecně*
- *Část 2: Mechanismy používající symetrické techniky*
- *Část 3: Mechanismy používající asymetrické techniky*

Úvod

Cílem služby nepopiratelnosti je vytvářet, shromažďovat, udržovat, zajistit dostupnost a ověřovat důkazy týkající se údajné události nebo činnosti, aby bylo možné řešit spory o tom, zda se událost nebo činnost vyskytla či nikoliv. Tato část ISO/IEC 13888 definuje model mechanismů nepopiratelnosti poskytujících důkazy, které jsou založeny na kryptografických kontrolních hodnotách, vytvářených pomocí symetrických nebo asymetrických kryptografických technik.

Služby nepopiratelnosti zajišťují důkaz; důkaz zajišťuje (jednoznačnou) odpovědnost ve vztahu k jednotlivé události nebo činnosti. Entita odpovědná za danou činnost nebo spojená s danou událostí, vzhledem k níž je generován důkaz, je označována jako subjekt důkazu.

Mechanismy nepopiratelnosti poskytují protokoly pro výměnu tokenů nepopiratelnosti specifických pro každou službu nepopiratelnosti. Tokeny nepopiratelnosti sestávají z bezpečných obálek a/nebo digitálních podpisů a volitelně doplňkových dat:

- Bezpečné obálky jsou vytvářené autoritou generující důkaz s použitím symetrických kryptografických technik.
- Digitální podpisy jsou vytvářeny generátorem důkazu nebo autoritou generující důkaz s použitím asymetrických kryptografických technik.

Tokeny nepopiratelnosti mohou být uchovávány jako informace nepopiratelnosti, která může být následně použita stranami, jež jsou ve sporu, nebo rozhodcem k rozhodování ve sporech.

V závislosti na politice nepopiratelnosti, účinné pro specifickou aplikaci, a právním prostředí, v jehož rámci aplikace pracuje, mohou být pro doplnění informace nepopiratelnosti požadovány dodatečné informace, například:

- důkaz obsahující důvěryhodné vyznačení času, poskytnuté autoritou pro vyznačování času,
- důkaz poskytnutý notářem, který poskytuje záruku týkající se vytvořených dat nebo činnosti či události uskutečněné jednou nebo více entitami.

Nepopiratelnost může být zajištěna pouze v kontextu jasně definované bezpečnostní politiky pro konkrétní aplikaci a její legislativní prostředí. Politiky nepopiratelnosti jsou popsány v ISO/IEC 10181-4.

Specifické mechanismy nepopiratelnosti, obecně použitelné pro různé služby nepopiratelnosti, jsou nejprve popsány a potom aplikovány na vybrané specifické služby nepopiratelnosti jako:

- nepopiratelnost původu,
- nepopiratelnost doručení,
- nepopiratelnost podání,
- nepopiratelnost přenosu.

Dodatečné služby nepopiratelnosti uvedené v této části ISO/IEC 13888 jsou:

- nepopiratelnost vytvoření,
- nepopiratelnost přijetí,
- nepopiratelnost znalosti,
- nepopiratelnost odeslání.

1 Předmět normy

Tato část ISO/IEC 13888 slouží jako obecný model pro následující části specifikující mechanismy nepopiratelnosti používající kryptografické techniky. ISO/IEC 13888 poskytuje mechanismy nepopiratelnosti pro následující fáze nepopiratelnosti:

- vytváření důkazu,
- přenos, uložení a vyhledávání důkazu, a
- ověření důkazu.

Rozhodování sporů leží mimo rozsah ISO/IEC 13888.